

IN THE U.S. PATENT AND TRADEMARK OFFICE

In re application of

Hiroshi SHIMIZU

Conf.

Application No. NEW NON-PROVISIONAL

Group

Filed April 20, 2004

Examiner

NETWORK ACCESS SYSTEM

CLAIM TO PRIORITY

Assistant Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

April 20, 2004

Sir:

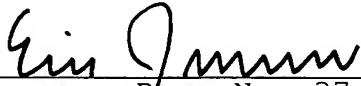
Applicant(s) herewith claim(s) the benefit of the priority filing date of the following application(s) for the above-entitled U.S. application under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55:

<u>Country</u>	<u>Application No.</u>	<u>Filed</u>
JAPAN	2003-115618	April 21, 2003

Certified copy(ies) of the above-noted application(s) is(are) attached hereto.

Respectfully submitted,

YOUNG & THOMPSON


Eric Jensen, Reg. No. 37,855
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
703) 979-4709

EJ/ia

Attachment(s): 1 Certified Copy(ies)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

2003年 4月21日

出願番号
Application Number:

特願 2003-115618

[ST. 10/C] :

[JP 2003-115618]

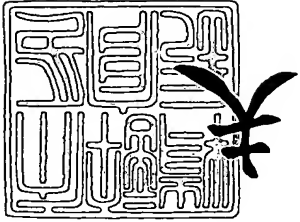
出願人
Applicant(s):

日本電気株式会社

特許庁長官
Commissioner,
Japan Patent Office

今井 康

2004年 4月 6日



出証番号 出証特 2004-3028167

【書類名】 特許願

【整理番号】 56200024

【提出日】 平成15年 4月21日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/56
H04L 12/28

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 清水 洋

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100123788

【弁理士】

【氏名又は名称】 宮崎 昭夫

【電話番号】 03-3585-1882

【選任した代理人】

【識別番号】 100088328

【弁理士】

【氏名又は名称】 金田 暢之

【選任した代理人】

【識別番号】 100106297

【弁理士】

【氏名又は名称】 伊藤 克博

【選任した代理人】

【識別番号】 100106138

【弁理士】

【氏名又は名称】 石橋 政幸

【手数料の表示】

【予納台帳番号】 201087

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0304683

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワークアクセスシステム

【特許請求の範囲】

【請求項 1】 複数のサブネットワークと、

前記複数のサブネットワークのうちのサブネットワーク内のクライアントのクライアント端末と当該クライアントがターゲットとする他のサブネットワークとの間のパケット通信用の通信セッションの開設に際し、当該クライアントの認証要求に応じて当該クライアントの認証を行う認証サーバと、

前記認証サーバによる認証後に当該認証サーバからの指示に基づいて、前記クライアント端末と前記クライアントがターゲットとするサブネットワークとの間のパケット通信に係るパケット信号のアドレス処理を行うアドレス処理回路とを有することを特徴とするネットワークアクセスシステム。

【請求項 2】 前記クライアントからの認証要求には、当該クライアントがターゲットとするサブネットワークの情報が含まれていることを特徴とする、請求項 1 に記載のネットワークアクセスシステム。

【請求項 3】 前記認証サーバは、前記クライアント毎に当該クライアントがターゲットとする 1 つまたは複数のサブネットワークを示す対応表を有し、前記対応表に基づいて前記クライアントがターゲットとするサブネットワークを特定すると共に、前記パケット信号上の前記通信セッションを特定する情報と前記クライアントがターゲットとするサブネットワークに対応するアドレス情報との対応を示すアドレス変換テーブルを前記アドレス処理装置内に設定することを特徴とする、請求項 1 または 2 に記載のネットワークアクセスシステム。

【請求項 4】 前記クライアント端末は、宛先アドレスとして前記アドレス処理装置のアドレスを設定してパケット信号を送出し、

前記アドレス処理装置は、前記アドレス変換テーブル内の前記パケット信号上の前記通信セッションを特定する情報に基づいて前記クライアントがターゲットとするサブネットワークを特定し、特定したサブネットワークに対応するアドレス情報に前記パケット信号の宛先アドレスを変換することを特徴とする、請求項 3 に記載のネットワークアクセスシステム。

【請求項 5】 前記パケット信号上の前記通信セッションを特定する情報として、発信アドレスを用いることを特徴とする、請求項 3 または 4 に記載のネットワークアクセスシステム。

【請求項 6】 前記通信セッションを特定する情報または当該情報の一部として、前記パケット信号上にセッション識別情報を設定することを特徴とする、請求項 5 に記載のネットワークアクセスシステム。

【請求項 7】 前記アドレス処理装置は、前記クライアントがターゲットとするサブネットワークから前記クライアント宛のパケット信号を受信した場合、当該パケット信号の発信アドレスを自己のアドレスに変換して送出することを特徴とする、請求項 1 から 6 のいずれか 1 項に記載のネットワークアクセスシステム。

【請求項 8】 前記サブネットワークは、ゲートウェイ装置を有し、当該サブネットワークに対応するアドレスとして前記ゲートウェイ装置のアドレスを用いることを特徴とする、請求項 1 から 7 のいずれか 1 項に記載のネットワークアクセスシステム。

【請求項 9】 前記ゲートウェイ装置および前記クライアント端末は、アドレスを記述したカプセル化ヘッダを付加してカプセル化したパケット信号のトンネル通信機能を有し、

前記ゲートウェイ装置は、自己のゲートウェイ装置宛のパケット信号から前記カプセル化ヘッダを除去して自己のサブネットワークに供給することを特徴とする、請求項 8 に記載のネットワークアクセスシステム。

【請求項 10】 前記ゲートウェイ装置は、自己のゲートウェイ装置宛のパケット信号の前記カプセル化ヘッダ内の発信アドレスと自己のネットワーク内で前記クライアント端末に割り当てられたアドレスとを対応付けて記録し、当該アドレスを宛先アドレスとするパケット信号を自己のサブネットワーク内で検出した場合、当該パケット信号の宛先アドレスとして当該アドレスに対応付けられた前記カプセル化ヘッダ内の発信アドレスを設定すると共に当該パケット信号の発信アドレスとして自己のアドレスを設定してカプセル化し、送出することを特徴とする、請求項 9 に記載のネットワークアクセスシステム。

【請求項 1 1】 前記サブネットワークの一部は、複数の前記認証サーバに接続されると共に、プロキシ認証サーバを有しており、

前記クライアント端末は、前記プロキシ認証サーバにアクセスして前記クライアントの認証要求を行い、

前記プロキシ認証サーバは、前記クライアントからの認証要求に基づき前記クライアントがターゲットとするサブネットワークが有する認証サーバを特定し、特定した認証サーバに対し認証の可否を問い合わせ、当該認証サーバに前記クライアントが認証された場合、当該クライアントのアクセスを許可することを特徴とする、請求項 1 から 1 0 のいずれか 1 項に記載のネットワークアクセスシステム。

【請求項 1 2】 前記認証サーバは、直接あるいはプロキシ認証サーバを介して認証されたクライアントのクライアント端末に対し、前記通信セッションを特定するためのセッション識別情報を配布し、

前記クライアント端末は、前記認証サーバから配布された前記セッション識別情報をパケット信号に付加することを特徴とする、請求項 6 または 1 1 に記載のネットワークアクセスシステム。

【請求項 1 3】 前記認証サーバは、前記クライアントの認証時に、当該クライアントのクライアント端末に対し、アクセスすべき前記アドレス処理装置のアドレスを通知し、

前記クライアント端末は、前記認証サーバから通知された前記アドレス処理装置を介して前記クライアントがターゲットとするサブネットワークとパケット通信を行うことを特徴とする、請求項 1 から 1 2 のいずれか 1 項に記載のネットワークアクセスシステム。

【請求項 1 4】 前記サブネットワークは、前記クライアントとして位置付けられるゲートウェイ装置を有し、

前記ゲートウェイ装置は、自己のサブネットワーク内のクライアントがターゲットとするサブネットワークとの間でカプセル化したパケット信号のトンネル通信を行い、自己のサブネットワーク内のクライアントからの通信セッションの開設のための認証要求を受け付けた場合、前記クライアントに代わって前記認証サ

ーバに当該クライアントの認証要求を行い、前記パケット信号上の前記通信セッションを特定する情報または当該情報の一部として、前記通信セッションを特定するためのセッション識別情報を用いることを特徴とする、請求項 1 から 13 のいずれか 1 項に記載のネットワークアクセスシステム。

【請求項 15】 前記認証サーバは、前記ゲートウェイ装置からの前記クライアントの認証要求に対し、当該クライアントがターゲットとするサブネットワークのアドレスを特定するための情報を前記ゲートウェイ装置に通知し、

前記ゲートウェイ装置は、前記認証サーバから通知された前記情報に基づいて前記クライアントがターゲットとするサブネットワーク宛のパケット信号を検出した場合、当該パケット信号の発信アドレスによりクライアントを特定し、特定したクライアントが前記通信セッションの開設のための認証を受けていることを確認すると、前記セッション識別情報をカプセル化ヘッダの一部に設定してパケット信号をカプセル化し、前記アドレス処理装置に送出することを特徴とする、請求項 14 に記載のネットワークアクセスシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、外部からターゲットネットワークに対しアクセスするためのネットワークアクセスシステムに関する。より具体的には、自部門ネットワークの外部から自部門ネットワークに対してアクセスするためのネットワークアクセスシステムに関する。

【0002】

【従来の技術】

従来のネットワークアクセスシステムについて、図 13 および図 14 を参照して説明する。

【0003】

図 13 を参照すると、本従来例は、インターネットなどのようにオープンにアクセスできるオープンネットワーク 1 と、企業内のローカルエリアネットワーク（基幹ネットワーク 12、リモートアクセス用ネットワーク 81、および部門ネ

ットワーク 83, 84) と、クライアントとターゲットネットワークとの間のパケット通信に係るパケット信号のアドレス処理を行うアドレス処理回路 13 とを設けた構成となっている。

【0004】

アドレス処理装置 13 は、基幹ネットワーク 12 およびオープンネットワーク 1 に接続されている。

【0005】

リモートアクセス用ネットワーク 81 は、ゲートウェイ (GW) 80 を有しており、GW 80 を介してアドレス処理装置 13 に接続されている。

【0006】

部門ネットワーク 83 は、ファイアウォール (FW) 82 を有しており、FW 82 を介して基幹ネットワーク 12 に接続されている。

【0007】

オープンネットワーク 1 は、オープンネットワーク 1 内のアクセス用アドレスをクライアントに割り当てる DHCP サーバ 5 を有している。

【0008】

以下、本従来例の動作について説明する。ここでは、オープンネットワーク 1 内のクライアント 2 が自部門ネットワーク (部門ネットワーク 83, 84 のいずれか) をターゲットネットワークとし、オープンネットワーク 1 からアクセスを行う場合の動作例について説明する。

【0009】

オープンネットワーク 1 内のクライアント 2 は、企業内のローカルエリアネットワーク内アクセス用のアドレスとして、リモートアクセス用ネットワーク 81 に対応したトンネル内 IP アドレス AD8X が割り当てられており、また、オープンネットワーク 1 内のアクセス用のアドレスとして、DHCP サーバ 5 によりアドレス AD02 が割り当てられている。

【0010】

クライアント 2 は、自部門ネットワーク (部門ネットワーク 83, 84 のいずれか) をターゲットネットワークとしてアクセスを行う場合、まず、自己のクラ

クライアント端末上で、パケット信号をカプセル化し、アドレス処理装置 13 に向けて送信する。

【0011】

具体的には、クライアント 2 は、図 14 中の (1) に示すように、トンネル発信アドレスとしてクライアント 2 のオープンネットワーク 1 内のアドレス AD02 を設定し、トンネル宛先アドレスとしてアドレス処理装置 13 のアドレス AD13 を設定したカプセル化ヘッダを付加してパケット信号をカプセル化し、カプセル化したパケット信号をアドレス処理装置 13 に向けて送信する。

【0012】

アドレス処理装置 13 は、トンネル宛先アドレスが AD13 であるパケット信号を受信すると、図 14 中の (2) に示すように、そのトンネル宛先アドレス AD13 を GW80 のアドレス AD80 に変換し、GW80 に転送する。

【0013】

GW80 は、上記で転送されたパケット信号からカプセル化ヘッダを除去して、オリジナルのパケット信号に復元した上で、そのパケット信号をリモートアクセス用ネットワーク 81 内に供給する。

【0014】

このとき、FWがない部門ネットワーク 84 に対してはパケット信号によるアクセスが可能であるが、FW82 を有する部門ネットワーク 83 へのアクセスを可能とするためには、FW82 に対して発信アドレスが AD8X であるパケット信号を通過させるような設定を行う必要がある。

【0015】

一方、オープンネットワーク 1 内のクライアント 2 へのパケット信号の通信は、その逆のプロセスを経て実現される。

【0016】

具体的には、GW80 は、クライアント 2 宛のパケット信号に対し、図 14 中の (3) に示すように、トンネル宛先アドレスとしてクライアント 2 のオープンネットワーク 1 内のアドレス AD02 を設定し、トンネル発信アドレスとして自己のアドレス AD80 を設定したカプセル化ヘッダを付加してカプセル化する。

【0017】

アドレス処理装置 13 は、図 14 中の (4) に示すように、GW80 からのパケット信号に設定されたトンネル発信アドレスを AD80 から自己のアドレスである AD13 に変換し、オープンネットワーク 1 へ送信する。

【0018】

なお、このようなネットワークアクセスシステムを実現するための技術としては、例えば、特許文献 1～3 に開示された技術が開示されている。

【0019】**【特許文献 1】**

特開 2001-160828 号公報

【特許文献 2】

特開 2001-186136 号公報

【特許文献 3】

特開 2001-274834 号公報

【0020】**【発明が解決しようとする課題】**

しかしながら、図 13 に示した従来のネットワークアクセスシステムにおいては、以下に記載するような課題がある。

【0021】

第 1 の課題は、クライアントが外部からファイアウォールで保護されている部門ネットワーク内のサーバ等にアクセスする場合、ファイアウォールに穴をあけてアクセスを行う必要があるが、クライアントの数が増大すると、ファイアウォールの穴の数が増大するため、各クライアントに対応した設定や運用管理が煩雑化してしまうということである。

【0022】

第 2 の課題は、ファイアウォールの穴は常にかいている状態であるため、セキュリティ面で脆弱になるということである。

【0023】

第 3 の課題は、パケット信号をカプセル化してトンネル型の通信を行う技術と

して、セキュリティ面をより嚴重にした I P s e c (IP Security) 技術があるが、I P s e c 技術を用いたトンネルを部門ネットワークまで伸張することができないということである。

【0024】

そこで、本発明の第1の目的は、クライアントの数が増大しても、各クライアントに対応した設定や運用管理をシンプルにすることができるネットワークアクセスシステムを提供することにある。

【0025】

また、本発明の第2の目的は、クライアントと部門ネットワーク内のサーバ等との間の上記の穴をあける設定を不要とすると共に、高いセキュリティ性を実現することができるネットワークアクセスシステムを提供することにある。

【0026】

さらに、本発明の第3の目的は、I P s e c 技術を用いたトンネルを部門ネットワークまで伸張することができるネットワークアクセスシステムを提供することにある。

【0027】

【課題を解決するための手段】

上記目的を達成するために本発明のネットワークアクセスシステムは、複数のサブネットワークと、前記複数のサブネットワークのうちのサブネットワーク内のクライアントのクライアント端末と当該クライアントがターゲットとする他のサブネットワークとの間のパケット通信用の通信セッションの開設に際し、当該クライアントの認証要求に応じて当該クライアントの認証を行う認証サーバと、前記認証サーバによる認証後に当該認証サーバからの指示に基づいて、前記クライアント端末と前記クライアントがターゲットとするサブネットワークとの間のパケット通信に係るパケット信号のアドレス処理を行うアドレス処理回路とを有することを特徴としている。

【0028】

したがって、クライアントからのパケット信号の宛先を当該クライアントがターゲットとするサブネットワークまで伸張することが可能となるため、トンネル

型通信を行う場合も、ターゲットとするサブネットワークまで IP トンネルを伸張することが可能となる。

【0029】

【発明の実施の形態】

以下に、本発明の実施の形態について図面を参照して説明する。

【0030】

（第 1 の実施形態）

本発明の第 1 の実施形態によるネットワークアクセスシステムについて、図 1 および図 2 を参照して説明する。

【0031】

図 1 を参照すると、本実施形態は、インターネットなどのようにオープンにアクセスできるオープンネットワーク 1 と、企業内の基幹ネットワーク 12 および部門ネットワーク 22, 32, 42 と、ターゲットネットワーク外部のクライアントとターゲットネットワークとの間のパケット通信用の通信セッションの開設に際し、クライアントの認証要求に応じてクライアントの認証を行う認証サーバ 10 と、認証サーバ 10 による認証後に認証サーバ 10 からの指示に基づいて、クライアントとターゲットネットワークとの間のパケット通信に係るパケット信号のアドレス処理を行うアドレス処理回路 11 とを設けた構成となっている。

【0032】

アドレス処理装置 11 は、基幹ネットワーク 12 およびオープンネットワーク 1 に接続されており、さらに、基幹ネットワーク 12 を介してゲートウェイ（GW）22, 32, 42 に接続されている。なお、アドレス処理装置 11 は、基幹ネットワーク 12 を介さず、直接 GW 21, 31, 41 に接続されることとしても良い。

【0033】

認証サーバ 10 は、アドレス処理装置 11 を介してオープンネットワーク 1 および基幹ネットワーク 12 に接続されている。なお、認証サーバ 10 は、アドレス処理装置 11 を介さず、直接オープンネットワーク 1 および基幹ネットワーク 12 に接続されることとしても良い。

【0034】

各部門ネットワーク 22, 32, 42 は、GW21, 31, 41 を有しており、GW21, 31, 41 を介して基幹ネットワーク 12 に接続されている。

【0035】

オープンネットワーク 1 は、オープンネットワーク 1 内のアクセス用アドレスをクライアントに割り当てる DHCP サーバ 5 を有しており、また、各部門ネットワーク 32, 42 は、部門ネットワーク 32, 42 内のアクセス用アドレスをクライアントに割り当てる DHCP サーバ 35, 45 を有している。

【0036】

以下、本実施形態の動作について説明する。本実施形態は、オープンネットワーク 1 内のクライアントが、自部門ネットワークをターゲットネットワークとしてアクセスを行う場合に適用される。ここでは、部門ネットワーク 32 に属するクライアント 3 が部門ネットワーク 32 をターゲットネットワークとし、オープンネットワーク 1 からアクセスを行う場合の動作例について説明する。

【0037】

図 2 を参照すると、まず、クライアント 3 は、自己のクライアント端末上で、DHCP サーバ 5 によりオープンネットワーク 1 内のアクセス用のアドレス AD03 の割り当てを受ける。

【0038】

続いて、クライアント 3 は、自己のクライアント端末上で、認証サーバ 10 に認証のためのアクセスを行う。このアクセスに際しては、クライアント 3 は、クライアント 3 を特定するためのクライアント特定情報（例えば、ログインネーム（ユーザネーム））やパスワードを認証サーバ 10 に入力する。

【0039】

認証サーバ 10 は、クライアント 3 から入力されたクライアント特定情報およびパスワードに基づいてクライアント 3 の認証を行った後、クライアント 3 が属する部門ネットワーク 32 を特定する。なお、認証サーバ 10 は、クライアント特定情報とそのクライアント特定情報により特定されるクライアントの属する部門ネットワークとの対応表を有しており、この対応表を用いてクライアント 3 が

属する部門ネットワーク 32 を特定する。一つのクライアントに複数のターゲットネットワークが登録されている場合は、認証要求にターゲットネットワーク情報を加えるか、ユーザネームを違えるなどして、クライアント特定情報をターゲットネットワークに応じて複数設定すれば良い。

【0040】

次に、認証サーバ 10 は、図 3 に示すように、上記で特定した部門ネットワーク 32 が有する GW 31 のアドレス AD 31 と、クライアント 3 のオープンネットワーク 1 内のアドレス AD 03 とを対応付けたアドレス変換テーブルをアドレス処理装置 11 の内部に設定する。

【0041】

クライアント 3 は、認証サーバ 10 による認証がなされると、続いて、自己のクライアント端末上で、アドレス処理装置 11 を介して GW 31 との間にトンネルを設定し、カプセル化したパケット信号のトンネル型通信を行う。

【0042】

具体的には、クライアント 3 は、図 4 中の (1) に示すように、トンネル発信アドレスとしてクライアント 3 のオープンネットワーク 1 内のアドレス AD 03 を設定し、トンネル宛先アドレスとしてアドレス処理装置 11 のアドレス AD 11 を設定したカプセル化ヘッダを付加してパケット信号をカプセル化し、カプセル化したパケット信号をアドレス処理装置 11 に向けて送信する。

【0043】

アドレス処理装置 11 は、クライアント 3 からのパケット信号を受信すると、図 3 のアドレス変換テーブルを参照し、パケット信号に設定された発信アドレス AD 03 に GW 31 のアドレス AD 31 が対応付けられていることを認識する。

【0044】

この結果、アドレス処理装置 11 は、図 4 中の (2) に示すように、クライアント 3 からのパケット信号のトンネル宛先アドレス AD 11 を GW 31 のアドレス AD 31 に変換し、基幹ネットワーク 12 に送信する。この処理により、クライアント 3 とアドレス処理装置 11 との間に設定されたトンネルは GW 31 まで伸張されることになる。

【0045】

GW31は、クライアント3からのパケット信号からカプセル化ヘッダを除去してオリジナルのパケット信号に復元した上で、そのパケット信号を部門ネットワーク32内に供給する。このようにして、クライアント3は、図1中の部門ネットワーク32内の黒四角マークに示すように、あたかも部門ネットワーク32内に存在しているようにして、部門ネットワーク32内の他のクライアントと通信を行うことができるようになる。

【0046】

続いて、DHCPサーバ35は、クライアント3とGW31との間に設定されたトンネルを介して、クライアント3に部門ネットワーク32内のアドレスAD3Xを割り当てる。また、GW31は、クライアント3の発信アドレスをモニタし、クライアント3のオープンネットワーク1内のアドレスがアドレスAD03であることを認識する。さらに、GW31は、クライアント3のオープンネットワーク1内のアドレスAD03と、DHCPサーバ35がクライアント3に割り当てた部門ネットワーク32内のAD3Xとを対応付けて記録する。

【0047】

その後、部門ネットワーク32からGW31を介したオープンネットワーク1内のクライアント3への通信は、その逆のプロセスを経て実現される。

【0048】

具体的には、GW31は、部門ネットワーク32内でクライアント3のアドレスAD3Xを宛先アドレスとするパケット信号を検出すると、図4中の(3)に示すように、トンネル宛先アドレスとしてクライアント3のオープンネットワーク1内のアドレスAD03を設定し、トンネル発信アドレスとして自己のアドレスAD31を設定したカプセル化ヘッダを付加してパケット信号をカプセル化し、基幹ネットワーク12に向けて送信する。

【0049】

上記のパケット信号は、企業内の基幹ネットワーク12および部門ネットワーク22, 32, 42のアドレスドメインには無いアドレスAD03を宛先アドレスとしているため、基幹ネットワーク12内のルーティング処理によってアドレ

ス処理装置 11 に転送される。

【0050】

アドレス処理装置 11 は、図 4 中の (4) に示すように、上記で転送されてきたパケット信号に設定されたトンネル発信アドレスを AD 31 から自己のアドレスである AD 11 に変換し、オープンネットワーク 1 へ送信する。

【0051】

なお、本実施形態においては、クライアント 3 に対し、オープンネットワーク 1 内のアドレス AD 03 や、部門ネットワーク 32 内のアドレス AD 3X を、固定的に割り当てることとしても良い。

【0052】

また、アドレス処理装置 11 は、アドレス変換テーブルに無いクライアントからの通信、即ち、未認証のアクセスは禁止することができ、かつ、認証サーバ 10 による認証時にアドレス変換テーブルが登録されるため、アドレス変換テーブルを予め設定しておく必要はない。

【0053】

また、アドレス処理装置 11 は、あるクライアントの通信が終了したことを検出した場合、その通信に係るクライアントのアドレス情報をアドレス変換テーブルから消去することとしても良い。この場合、アドレス処理装置 11 を介したアクセスが不可能となるため、セキュリティを高めることができる。

【0054】

また、クライアントと部門ネットワーク 22, 32, 42 の GW 21, 31, 32 間で IPsec 技術を用い、トンネルの中は暗号化されたパケット信号が流れるようにしても良い。

【0055】

また、GW 21, 31, 32 にとってもアドレス処理装置 11 を介さないクライアントからの部門ネットワーク 22, 32, 42 へのアクセスは禁止できるので、高いセキュリティを維持することができる。

【0056】

(第 2 の実施形態)

本発明の第2の実施形態によるネットワークアクセスシステムについて、図1を参照して説明する。

【0057】

本実施形態は、同一企業内の他部門ネットワーク内のクライアントが、自部門ネットワークをターゲットネットワークとしてアクセスを行う場合に適用される。なお、本実施形態の構成は、図1と同様の構成であるため、説明を省略する。

【0058】

以下、本実施形態の動作について説明する。ここでは、部門ネットワーク32の部門に属するクライアント4が部門ネットワーク32をターゲットネットワークとし、部門ネットワーク42からアクセスを行う場合の動作例について説明する。

【0059】

まず、クライアント4は、自己のクライアント端末上で、DHCPサーバ45により部門ネットワーク42内のアクセス用のアドレスAD43の割り当てを受け、続いて、認証サーバ10に認証のためのアクセスを行う。

【0060】

認証サーバ10は、クライアント4の認証を行った後、クライアント4が属する部門ネットワーク32を特定し、図3に示すように、クライアント4の部門ネットワーク42内のアドレスAD43と、GW31のアドレスAD31とを対応付けたアドレス変換テーブルをアドレス処理装置11の内部に設定する。

【0061】

クライアント4は、認証サーバ10による認証がなされると、続いて、自己のクライアント端末上で、アドレス処理装置11のアドレスAD11をトンネル宛先アドレスとして設定し、クライアント4の部門ネットワーク42内のアドレスAD43をトンネル発信アドレスとして設定したカプセル化ヘッダをパケット信号に付加してカプセル化し、カプセル化したパケット信号をアクセス処理装置11に向けて送出する。

【0062】

アドレス処理装置11は、クライアント4からのパケット信号を受信すると、

図 3 のアドレス変換テーブルを参照し、クライアント 4 からのパケット信号のトンネル宛先アドレス AD 1 1 を GW 3 1 のアドレス AD 3 1 に変換し、パケット信号を GW 3 1 に中継転送する。

【0063】

一方、部門ネットワーク 3 2 から部門ネットワーク 4 2 内のクライアント 4 への通信は、その逆のプロセスを経て実現される。

【0064】

具体的には、GW 3 1 は、部門ネットワーク 3 2 内でクライアント 4 を宛先とするパケット信号を検出すると、トンネル宛先アドレスとしてクライアント 4 の部門ネットワーク 4 2 内のアドレス AD 4 3 を設定し、トンネル発信アドレスとして自己のアドレス AD 3 1 を設定したカプセル化ヘッダを付加してパケット信号をカプセル化し、カプセル化したパケット信号を基幹ネットワーク 1 2 に送信する。

【0065】

上記のパケット信号は、企業内の部門ネットワーク 4 2 内のアドレス AD 4 3 を宛先アドレスとしているため、基幹ネットワーク 1 2 内のルーティング処理によりアドレス処理装置 1 1 を介さずに直接部門ネットワーク 4 2 に転送される。

【0066】

なお、本実施形態においては、企業内アクセスがプライベートアドレスであり、オープンネットワーク 1 がグローバルアドレスである場合には、アドレス処理装置 1 1 はそれぞれのアドレスを持つことになる。すなわち、オープンネットワーク 1 内のクライアント 2, 3 がアクセスするアドレス処理装置 1 1 のアドレスはグローバルアドレスとなり、他の部門ネットワーク 4 2 内のクライアント 4 がアクセスするアドレス処理装置 1 1 のアドレスは企業内アドレスとなる。

【0067】

(第 3 の実施形態)

本発明の第 3 の実施形態によるネットワークアクセスシステムについて、図 1 を参照して説明する。

【0068】

本実施形態は、あるクライアントが外部から自部門ネットワークをターゲットネットワークとしてアクセスを行う際に、パケット信号をカプセル化せずにアクセスを行う場合に適用される。なお、本実施形態の構成は、図 1 と同様の構成であるため、説明を省略する。

【 0 0 6 9 】

以下、本実施形態の動作について説明する。ここでは、部門ネットワーク 2 2 の部門に属するクライアント 2 が部門ネットワーク 2 2 をターゲットネットワークとし、オープンネットワーク 1 からパケット信号をカプセル化せずにアクセスを行う場合の動作例について説明する。

【 0 0 7 0 】

認証サーバ 1 0 は、クライアント 2 の認証を行った後、クライアント 2 が属する部門ネットワーク 2 2 を特定し、図 3 に示すように、クライアント 2 のオープンネットワーク 1 内のアドレス A D 0 2 と、部門ネットワーク 2 2 の外部からのアクセスに対する通信専用のサーバ 2 0 のアドレス A D 2 0 とを対応付けたアドレス変換テーブルをアドレス処理装置 1 1 の内部に設定する。

【 0 0 7 1 】

クライアント 2 は、認証サーバ 1 0 による認証がなされると、続いて、自己のクライアント端末上で、図 5 中の (1) に示すように、アドレス処理装置 1 1 のアドレス A D 1 1 を宛先アドレスとして、パケット信号を送信する。

【 0 0 7 2 】

アドレス処理装置 1 1 は、クライアント 2 からのパケット信号を受信すると、図 3 のアドレス変換テーブルを参照し、図 5 中の (2) に示すように、クライアント 2 からのパケット信号の宛先アドレスをサーバ 2 0 のアドレス A D 2 0 に変換し、パケット信号を G W 2 1 に中継転送し、G W 2 1 は、パケット信号に設定されたアドレス A D 2 0 に基づきパケット信号をサーバ 2 0 に転送する。

【 0 0 7 3 】

これにより、クライアント 2 は、固定的ではあるが、サーバ 2 0 に接続できるようになる。このように、カプセル化技術を用いなくても、部門ネットワーク 2 2 の外部からのアクセスに対する通信専用のサーバ 2 0 を用意しておけば、外部

から部門ネットワーク 22 内へのアクセスが可能となり、また、部門ネットワーク 22 内の他の資源へのアクセスを禁止することも可能となる。

【0074】

一方、サーバ 20 からオープンネットワーク 1 内のクライアント 2 への通信は、その逆のプロセスを経て実現される。図 5 中の (3) に、サーバ 20 からアドレス処理装置 11 までのパケット信号に設定されたアドレスヘッダを示し、図 5 中の (4) に、アドレス処理装置 11 からクライアント 2 までのパケット信号に設定されたアドレスヘッダを示す。

【0075】

なお、本実施形態においては、GW 21 には、部門ネットワーク 22 の外部からのアクセスがあった場合は、そのアクセスをサーバ 20 に限定して転送するように設定することとしても良い。その場合にも、部門ネットワーク 22 内の他の資源へのアクセスを禁止することが可能となる。

【0076】

(第 4 の実施形態)

本発明の第 4 の実施形態によるネットワークアクセスシステムについて、図 6 を参照して説明する。

【0077】

図 6 を参照すると、本実施形態においては、部門ネットワーク 52 が、モバイル IP を用いたホームエージェント (HA) 51 を介して基幹ネットワーク 12 に接続された構成となっている。

【0078】

モバイル IP プロトコルを用いたパケット信号も、図 4 に示すようにカプセル化された構造となっている。そのため、トンネルを終端する GW 31 の代わりに HA 51 を配置すれば、第 1 の実施形態と同様にして、モバイル IP によるトンネルを部門ネットワーク 52 まで伸張させることが可能となる。

【0079】

すなわち、本実施形態においては、認証サーバ 10 による認証がなされた、部門ネットワーク 52 に属するクライアントは、オープンネットワーク 1 にいよう

が（クライアント 2, 3）、他の部門ネットワーク 32, 42（クライアント 4）にしようが、自己のクライアント端末上で H A 5 1 にアクセスできるので、H A 5 1 に接続された部門ネットワーク 52 をベースとしてモバイルサービスを受けることができる。

【0080】

なお、本実施形態においては、クライアントと GW とのエンド間のカプセル化プロトコルそのものの種類や方式を限定する訳ではないので、カプセル化したパケット信号を通信する一般的な通信方式に適用可能である。

【0081】

（第 5 の実施形態）

本発明の第 5 の実施形態によるネットワークアクセスシステムについて、図 7 を参照して説明する。

【0082】

図 7 を参照すると、本実施形態においては、部門ネットワーク 62 が、GW 61 および他の部門ネットワーク 32 を介して基幹ネットワーク 12 に接続された構成となっている。

【0083】

本実施形態においては、部門ネットワーク 62 に属するクライアントからのトンネルは、GW 31 を通過し GW 61 まで伸張される。なお、GW 61 までトンネルを伸張するためには、GW 31 に対し、GW 61 を宛先とするパケット信号については通過させるよう設定すれば良いため、パケット信号が通過する部門ネットワーク 32 のセキュリティ面が脆弱になることはない。

【0084】

すなわち、本実施形態においては、各ネットワークがルーティング機能を有していれば、部門ネットワーク 62 に属するクライアントは、オープンネットワーク 1 にしようが（クライアント 2, 3）、他部門ネットワーク 32, 42 にしようが、基幹ネットワーク 12（クライアント 15）にしようが、認証サーバ 10 による認証を受けた後に、自己のクライアント端末上で自部門の部門ネットワーク 62 にアクセスすることができる。

【0085】

なお、本実施形態においては、必要に応じて、基幹ネットワーク12が、基幹ネットワーク12内のアクセス用アドレスをクライアントに割り当てるDHCPサーバを有することとしても良い。

【0086】

(第6の実施形態)

本発明の第6の実施形態によるネットワークアクセスシステムについて、図8を参照して説明する。

【0087】

図8を参照すると、本実施形態においては、認証サーバ10の配下に、複数のアドレス処理装置11、14が設けられた構成となっている。

【0088】

部門ネットワーク22、32は、GWや基幹ネットワークを介さずに直接アドレス処理装置11に接続されており、また、部門ネットワーク42は、GWや基幹ネットワークを介さずに直接アドレス処理装置14に接続されている。

【0089】

本実施形態においては、認証サーバ10は、オープンネットワーク1内のクライアント4を認証すると、クライアント4から入力されたクライアント特定情報に基づきクライアント4が属する部門ネットワーク42を特定する。そして、特定した部門ネットワーク42に接続されているアドレス処理装置14のアドレスであるAD14をクライアント4に通知する。

【0090】

クライアント4は、自己のクライアント端末上で、認証サーバ10から通知されたアドレス処理装置14のAD14を宛先アドレスとしてパケット信号をパケット化し、第1の実施形態と同じようにして、リモートアクセスを行う。

【0091】

(第7の実施形態)

本発明の第7の実施形態によるネットワークアクセスシステムについて、図9を参照して説明する。

【0092】

図9を参照すると、本実施形態においては、アクセスネットワーク6内のクライアントが、基幹ネットワーク9を介して複数の企業ネットワーク111, 121, 131にアクセスする構成となっている。

【0093】

アクセスネットワーク6は、クライアントのアクセスを制御するアクセスゲート7とプロキシ認証サーバ8を有しており、基幹ネットワーク9を介し複数の企業ネットワーク111, 121, 131に接続されている。

【0094】

企業ネットワーク111は、認証サーバ110を有している。さらに、企業ネットワーク111は、IPトンネルを終端するGW113を有しており、GW113および基幹ネットワーク9を介してアクセスネットワーク6に接続されている。

【0095】

企業ネットワーク121は、部門ネットワーク124, 126から構成されると共に、認証サーバ120を有している。部門ネットワーク124, 126は、IPトンネルを終端するGW123, 125を有しており、GW123, 125および基幹ネットワーク9を介してアクセスネットワーク6に接続されている。

【0096】

企業ネットワーク131は、部門ネットワーク134, 136から構成されると共に、認証サーバ130およびアドレス処理装置132を有している。部門ネットワーク134, 136は、IPトンネルを終端するGW133, 135を有しており、GW123, 125、アドレス処理装置132および基幹ネットワーク9を介してアクセスネットワーク6に接続されている。

【0097】

なお、各企業ネットワーク111, 121, 131とアクセスゲート7との接続は、基幹ネットワーク9上の仮想プライベートネットワークにより実現されるものとする。

【0098】

以下、本実施形態における動作例として、アクセスネットワーク 6 内のクライアント 2 からの 3 つのアクセス形態の各動作例について説明する。

【0099】

最初に、企業ネットワーク 111 に属するクライアント 2 が企業ネットワーク 111 をターゲットネットワークとし、アクセスネットワーク 6 からアクセスを行う場合の動作例について説明する。

【0100】

クライアント 2 は、まず、自己のクライアント端末上で、クライアント 2 を特定するためのクライアント特定情報（例えば、Username@company#name）やパスワードを入力して、プロキシ認証サーバ 8 に認証のためのアクセスを行う。

【0101】

プロキシ認証サーバ 8 は、クライアント 2 のクライアント特定情報（例えば、Username@company#name）のうち所属企業を示す情報（この場合、ドメインネームである company#name）に基づきクライアント 2 が企業ネットワーク 111 に属することを認識し、企業ネットワーク 111 に設けられた認証サーバ 110 に認証の可否を問い合わせる。

【0102】

プロキシ認証サーバ 8 は、認証サーバ 110 により認証を示す通知を受けると、アクセスゲート 7 に対し、クライアント 2 からの通信を可能とする設定を行うよう指示する。この制御により、クライアント 2 は、アクセスゲート 7 と GW 113 との間をつなぐ基幹ネットワーク 9 上の仮想プライベートネットワークにログインすることになる。

【0103】

アクセスゲート 7 は、プロキシ認証サーバ 8 からの指示に基づき、クライアント 2 からのパケット信号の宛先アドレスを GW 113 宛のアドレスに変換する。

【0104】

なお、GW 113 は、企業ネットワーク 111 内に設けられているので、GW 113 のアドレスがプライベートアドレスの場合もある。

【0105】

次に、企業ネットワーク 131 に属するクライアント 2 が企業ネットワーク 131 をターゲットネットワークとし、アクセスネットワーク 6 からアクセスを行う場合の動作例について説明する。

【0106】

プロキシ認証サーバ 8 は、クライアント 2 のクライアント特定情報に基づきクライアント 2 が企業ネットワーク 131 に属することを認識すると、企業ネットワーク 131 に設けられた認証サーバ 130 に認証の可否を問い合わせる。

【0107】

プロキシ認証サーバ 8 は、認証サーバ 130 により認証を示す通知を受けると、クライアント 2 からのパケット信号の宛先アドレスをアドレス処理装置 132 宛のアドレスに変換するようアクセスゲート 7 に指示し、アクセスゲート 7 は、クライアント 2 からのパケット信号に設定された宛先アドレスをアドレス処理装置 132 宛のアドレスに変換する。この制御により、例えば、クライアント 2 が部門ネットワーク 134 に属する場合、クライアント 2 からの IP トンネルは、アクセスゲート 7 およびアドレス処理装置 132 における IP アドレスの変換処理により中継され、GW 133 まで伸張されることになる。

【0108】

次に、企業ネットワーク 121 に属するクライアント 2 が企業ネットワーク 121 をターゲットネットワークとし、アクセスネットワーク 6 からアクセスを行う場合の動作例について説明する。

【0109】

プロキシ認証サーバ 8 は、クライアント 2 のクライアント特定情報に基づきクライアント 2 が企業ネットワーク 121 に属することを認識すると、企業ネットワーク 121 に設けられた認証サーバ 120 に認証の可否を問い合わせる。

【0110】

プロキシ認証サーバ 8 は、認証サーバ 120 により認証を示す通知を受けると同時に、クライアント 2 の属する部門ネットワークの GW の IP アドレスの通知を受ける。

【0111】

例えば、クライアント 2 が部門ネットワーク 124 に属する場合、プロキシ認証サーバ 8 は、GW 123 のアドレスが通知され、アクセスゲート 7 に対し、クライアント 2 からのパケット信号の宛先アドレスを GW 123 のアドレスに変換するよう指示し、アクセスゲート 7 は、クライアント 2 からのパケット信号の宛先アドレスを GW 123 宛のアドレスに変換する。この制御により、クライアント 2 からの IP トンネルは、GW 123 まで伸張されることになる。このように、アクセスゲート 7 に対し、企業ネットワーク 121 内の宛先を振り分ける機能を備えさせることが可能となる。

【0112】

(第 8 の実施形態)

本発明の第 8 の実施形態によるネットワークアクセスシステムについて、図 10 および図 11 を参照して説明する。

【0113】

図 10 を参照すると、本実施形態においては、クライアントが自部門ネットワークをターゲットネットワークとし、ネットワークアドレス変換装置 (Network Address Translator : NAT) を介してアクセスを行う構成となっている。

【0114】

NAT 46 は、サブネットワーク 45 をオープンネットワーク 1 に接続している。また、オープンネットワーク 1 には GW 48 を介してサブネットワーク 47 も接続されている。

【0115】

以下、本実施形態の動作について説明する。ここでは、サブネットワーク 45 内のクライアントが、サブネットワーク 45 から NAT 46 を介してアクセスを行う場合の動作例について説明する。

【0116】

サブネットワーク 45 内のクライアントから送信されたパケット信号の宛先となる IP アドレスは、NAT 46 において別のアドレスに変換され、オープンネットワーク 1 に送出される。

【0117】

このとき、NAT 46にて変換された後のIPアドレスをサブネットワーク45内の複数のクライアントで共有している場合、アドレス処理装置11にてターゲットネットワークを特定できない場合がある。

【0118】

その場合、図11に示すように、サブネットワーク45内のクライアントは、パケット信号のカプセル化に際し、カプセル化ヘッダ内にクライアントを特定するクライアント特定情報XIDを挿入する。

【0119】

アドレス処理装置11は、図3のアドレス処理装置11内のアドレス変換テーブルにおいて、発信アドレスの代わりに、クライアントを特定する情報として、発信アドレス+XID、またはXIDのみを用いれば、第1の実施形態と同様に、ターゲットネットワークを特定し、アクセスすることができる。

【0120】

一方、ターゲットネットワークのGWは、サブネットワーク45内のクライアントからのパケット信号を受信すると、受信したパケット信号中のXIDをそのままカプセル化ヘッダのXIDに挿入し、サブネットワーク45内のクライアントまたはGW48に対して送信することになる。

【0121】

上記のようにXIDを用いる方式は、1人のクライアントが複数の異なるターゲットネットワークに同時にアクセスする場合にも適用することができる。この場合、クライアント（オープンネットワーク1内のクライアントでも、サブネットワーク45内のクライアントでも良い）に複数のXIDを付与し、クライアントから認証サーバ10に対してターゲットネットワークの情報も付加して認証を受け、ターゲットネットワークに対応してXIDを割り付けるようにする。それにより、アドレス処理装置11にて複数の異なるターゲットネットワークを特定することができるため、クライアントは、同時に複数のターゲットネットワークにアクセスすることができる。

【0122】

さらに、NAT 46にて、サブネットワーク45内のクライアントから送信さ

れたパケット信号のトンネル発信アドレスを全て一律にAD46に変換する場合でも、アドレス処理装置11にてサブネットワーク45内の全てのトンネルセッションを特定できるようにXIDを割り付けるようにすれば、複数のクライアントが同時に複数の異なるターゲットネットワークにアクセスすることができる。

【0123】

なお、本実施形態においては、クライアントを特定するXID情報は予め固定的にクライアントに設定しても良く、また、認証時に認証サーバ10によりクライアントに割り当てることにも良い。

【0124】

また、同一クライアントが異なるターゲットネットワークにアクセスを行う場合、認証サーバ10による認証は、ユーザネームとターゲットネットワーク名とを組み合わせで行うか、ターゲットネットワーク毎に異なるユーザネームを設定して行えば良い。

【0125】

また、XIDの長さを十分に長くすれば、アドレス処理装置11にてXIDに基づいてアドレス変換を行うことができるが、XIDの成りすましに対する耐力を改善するためには、トンネル発信アドレス+XIDに基づいてアドレス変換を行うことが望ましい。

【0126】

(第9の実施形態)

本発明の第9の実施形態によるネットワークアクセスシステムについて、図10を参照して説明する。

【0127】

本実施形態は、クライアントが自部門ネットワークをターゲットネットワークとしアクセスを行う際に、GW間でIPトンネル制御を行う場合に適用される。なお、本実施形態の構成は、図10と同様の構成であるため、説明を省略する。

【0128】

以下、本実施形態の動作について説明する。ここでは、GW48と、基幹ネットワーク12上の部門ネットワーク22、32、42のいずれかであるターゲッ

トネットワークのGWとの間でIPトンネル制御を行う場合の動作例について説明する。

【0129】

まず、サブネットワーク47内のクライアントは、自己のクライアント端末上で、プロキシ認証サーバ（図9参照）機能を有するGW48に認証のためのアクセスを行う。

【0130】

GW48は、サブネットワーク47内のクライアントのアドレスとユーザネームとの対応を記録すると共に、自己のアドレスAD48を発信アドレスとしたパケット信号を認証サーバ10に転送することにより、このクライアントのユーザネームやパスワードを認証サーバ10に中継する。

【0131】

認証サーバ10は、サブネットワーク47内クライアントからGW48を中継した認証要求に基づく認証が可である場合、この認証要求に対するXIDと、GW48のアドレスであるAD48およびターゲットネットワークのGWのアドレスとをアドレス処理装置11内のアドレス変換テーブルに設定すると共に、ユーザネームとXIDとをGW48に通知する。

【0132】

GW48は、認証サーバ10から通知されたユーザネームに対応したクライアントからの他のサブネットワーク宛のパケット信号に対しては、図11に示すようにXIDを付加してカプセル化し、オープンネットワーク1に送出する。

【0133】

アドレス処理装置11は、クライアントからのパケット信号に設定されたトンネル発信アドレスAD48とXID情報とに基づいて、トンネル宛先アドレスをターゲットネットワークのGWのアドレスに変換し、パケット信号をターゲットネットワークのGWに転送する。

【0134】

このようにして、基幹ネットワーク12上のターゲットネットワークのGWとGW48との間でトンネル制御を実現することができるため、サブネットワーク

47内のクライアントは、そのクライアントに対応して設定されたターゲットネットワークにアクセスすることが可能となる。

【0135】

一方、ターゲットネットワークのGWは、サブネットワーク45内のクライアントからのパケット信号を受信すると、受信したパケット信号中のXIDをそのままカプセル化ヘッダのXIDに挿入し、サブネットワーク47内のクライアントまたはGW48に対して送信することになる。

【0136】

なお、サブネットワーク47内のクライアントが複数のターゲットネットワークにアクセスする場合には、以下のような処理を行えば良い。

【0137】

認証サーバ10は、認証時にターゲットネットワークを認識すると、ターゲットネットワークとして認識したサブネットワークのアドレスおよびアドレスマスクに対応するXIDをGW48に通知する。

【0138】

GW48は、サブネットワーク47内のクライアントからのパケット信号の宛先アドレスを監視し、アドレスマスクされたアドレスが、認証サーバ10による認証を受けた上述のサブネットワークのアドレスと一致しているか判断する。一致している場合は、アドレスマスクされたアドレスに対応するXIDを、図11に示したようにカプセル化ヘッダに挿入することで、カプセル化したパケット信号をオープンネットワーク1に送出する。

【0139】

このとき、XIDは、上記のように、認証サーバ10による認証時にGW48にXIDを通知することとしても良く、GW48に予め複数のXIDをプールしておくこととしても良い。この場合は、GW48は、認証サーバ10に対して、予めプールされている未使用のXIDを添付して認証要求を行うこととし、このXIDがアドレス処理装置11内のアドレス変換テーブルに登録される。

【0140】

なお、本実施形態においては、サブネットワーク45、47のアドレスおよび

ターゲットネットワークのアドレスをプライベートアドレスとし、オープンネットワーク 1 のアドレスをグローバルアドレスとするネットワーク構成にも適用することが可能である。

【0141】

また、X I D の長さを十分に長くすれば、アドレス処理装置 11 にて X I D に基づいてアドレス変換を行うことができるが、X I D の成りすましに対する耐力を改善するためには、トンネル発信アドレス + X I D に基づいてアドレス変換を行うことが望ましい。

【0142】

(第 10 の実施形態)

本発明の第 10 の実施形態によるネットワークアクセスシステムについて、図 12 を参照して説明する。

【0143】

図 12 を参照すると、本実施形態においては、クライアントが属する自部門ネットワークをターゲットネットワークとするのではなく、GW における I P トンネル制御を簡易にするために、クライアントが属する自部門ネットワークに対応付けされ、ネットワークアクセス専用を設定されたネットワークを、ターゲットネットワークとする構成となっている。

【0144】

部門ネットワーク 74 に属するクライアントには、リモートアクセス用のネットワーク (I P サブネットワーク) 75 が対応付けられており、クライアントのターゲットネットワークは、部門ネットワーク 74 ではなく、ネットワークアクセス用ネットワーク 75 となる。

【0145】

部門ネットワーク 74 は、ファイアウォール (FW) 72 およびルータ 73 を介して、アドレス処理装置 70 が設けられている外部ネットワーク (不図示) に接続されている。

【0146】

GW 71 は、アドレス処理装置 70 から転送されてきたカプセル化されたパケ

ット信号（カプセル化ヘッダの宛先アドレスはGW71）を受信すると、受信したパケット信号からカプセル化ヘッダを除去し、オリジナルのパケット信号に復元する。このオリジナルのパケット信号はルータ73を介して部門ネットワーク74に転送される。

【0147】

すなわち、外部ネットワーク内のクライアントは、部門ネットワーク74とはFW72を介さずに接続されるので、FW72を介さずに部門ネットワーク74にアクセスできる。

【0148】

リモートアクセス用のネットワーク75に属するネットワークアクセスクライアント宛のパケット信号は、部門ネットワーク74からルータ73を介してGW71に転送され、GW71にてカプセル化される。カプセル化されたパケット信号は、アドレス処理装置70に転送される。

【0149】

本実施形態においては、カプセル化処理をすべきパケット信号の振り分けをルータ73が行うことで、GW71でなすべき処理は、ネットワークにアクセスしたクライアントのパケット信号に対するカプセル化処理のみとなるので（IPsec技術を用いる場合は暗号化処理も行う）、GW71、FW72、ルータ73の各々の機能構成をシンプルにすることができる。

【0150】

なお、本実施形態においては、GW71、FW72、ルータ73の各々の機能を1つの装置に統合して実現することとしても良い。この場合でも、各々の構成要素の機能構成がシンプルであるため、各々の構成要素の機能を統合した1つの装置もシンプルにできる。

【0151】

なお、本発明は、クライアントの通信セッションの終了方法を特定するものではない。認証サーバは、例えば、クライアントとの間のログアウト手順により通信セッションの終了を検出した場合、その通信に係るクライアントのアドレス情報をアドレス変換テーブルから消去することとしても良い。それとは別に、直接

クライアントとの間で、Keep#Alive用の通信を行ったり、無通信状態のタイムアウト検出を行ったりすることにより、ログアウト手順を踏まえない通信セッションの終了、例えば、電源断やネットワークインタフェースカードの除去などによる通信セッションの終了にも対応できる。また、認証サーバは、各ネットワークのDHCPサーバと連携することにより、クライアントとの間のKeep-Alive通信やIPsecセッションのKeep#Alive用の通信を行うことによりクライアントの通信の終了を知ることができる。

【0152】

【発明の効果】

本発明は以上説明したように構成されているため、以下の（１）～（９）に記載するような効果を奏する。

（１）ターゲットとするサブネットワークに外部からアクセスするクライアントの認証を行う認証サーバと、認証サーバによる認証後に認証サーバからの指示に基づいてパケット通信に係るパケット信号のアドレス処理を行うアドレス処理回路とを設けた構成とすることにより、クライアントからのパケット信号の宛先を当該クライアントがターゲットとするサブネットワークまで伸張することができる。したがって、トンネル型通信を行う場合も、ターゲットとするサブネットワークまでIPトンネル（IPsecトンネル、モバイルIPトンネルを含む）を伸張することができる。

（２）サブネットワークへのパケット信号はファイアウォールを経由しないため、ファイアウォールに穴をあけてアクセスを行うための設定が不要になる。したがって、クライアントに対応するための設定が煩雑になることを回避できるだけでなく、高いセキュリティ性を維持することができる。

（３）クライアントは、自己が位置しているサブネットワーク内での自己のアドレスやアドレス処理装置のアドレスを設定するだけで良く、また、その設定を誤っても、その影響はターゲットとするサブネットワークのゲートウェイ装置とクライアントの間に限定され、ネットワーク全体に波及しない。

（４）ターゲットとするサブネットワーク内のアドレスの取得方法として、例えば、DHCP方式を採用する構成とすることにより、クライアント毎の設定は不

要となり、設定が簡便で設定誤りをすくなくすることができる。

(5) クライアントとターゲットとするサブネットワークのゲートウェイ装置と
の間のトンネルは、認証サーバにより認証された時しか提供されないので、高い
セキュリティを実現することができる。

(6) サブネットワークの一部が複数の認証サーバに接続されると共に、プロキ
シ認証サーバを設けた構成とすることにより、例えば、キャリアネットワーク内
の企業向け仮想ネットワークへのアクセスと仮想ネットワークから企業内ネット
ワークへのアクセスとを一度のログインで実現できる。

(7) クライアントの発信アドレスだけでなく、通信セッションを識別する識別
情報を付加しこの付加情報を用いて、クライアントがターゲットネットとするサ
ブネットワークの特定およびアドレス変換を行う構成とすることにより、複数の
クライアントが同時に複数の異なるターゲットネットワークにアクセスすること
ができる。また、クライアントは、途中にNATがあっても、ターゲットとする
サブネットワークまでIPトンネルを伸張することができる。

(8) サブネットワークがクライアントとして位置付けられるゲートウェイ装置
を設けた構成とすることにより、クライアントがゲートウェイの配下にある場合
にも、ターゲットネットワークにアクセスすることができ、クライアント毎に複
数のターゲットネットワークにアクセスすることもできる。

(9) 通信セッションは認証サーバにおいて管理されるので、ユーザ管理やアク
セス管理が可能となる。

【図面の簡単な説明】

【図 1】

本発明の第1から第3の実施形態によるネットワークアクセスシステムの構成
を示す図である。

【図 2】

本発明の第1の実施形態に係る通信手順を説明する図である。

【図 3】

図1に示したアドレス処理装置内のアドレス変換テーブルを示す図である。

【図 4】

本発明の第 1 の実施形態に係るカプセル化したパケット信号のアドレス変換処理を説明する図である。

【図 5】

本発明の第 3 の実施形態に係るカプセル化したパケット信号のアドレス変換処理を説明する図である。

【図 6】

本発明の第 4 の実施形態によるネットワークアクセスシステムの構成を示す図である。

【図 7】

本発明の第 5 の実施形態によるネットワークアクセスシステムの構成を示す図である。

【図 8】

本発明の第 6 の実施形態によるネットワークアクセスシステムの構成を示す図である。

【図 9】

本発明の第 7 の実施形態によるネットワークアクセスシステムの構成を示す図である。

【図 1 0】

本発明の第 8 および第 9 の実施形態によるネットワークアクセスシステムの構成を示す図である。

【図 1 1】

本発明の第 8 の実施形態に係るカプセル化したパケット信号の内容を説明する図である。

【図 1 2】

本発明の第 1 0 の実施形態によるネットワークアクセスシステムの構成を示す図である。

【図 1 3】

本従来例のネットワークアクセスシステムの構成を示す図である。

【図 1 4】

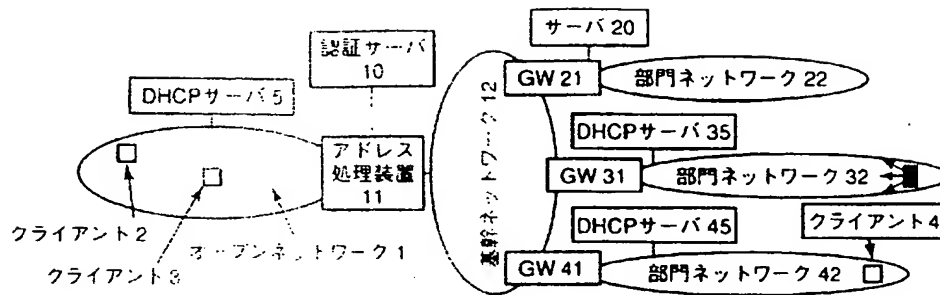
本従来例に係るカプセル化したパケット信号のアドレス変換処理を説明する図である。

【符号の説明】

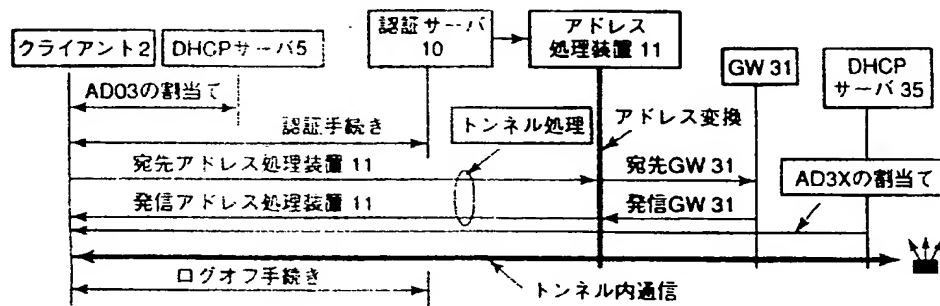
- 1 オープンネットワーク
- 2, 3, 4, 15 クライアント
- 5, 15, 35, 45 DHCPサーバ
- 6 アクセスネットワーク
- 7 アクセスゲート
- 8 プロキシ認証サーバ
- 9, 12 基幹ネットワーク
- 10, 110, 120, 130 認証サーバ
- 11, 12, 13, 112, 122, 132 アドレス処理装置
- 20 サーバ
- 21, 31, 41, 48, 61, 71, 80, 113, 123, 125, 133, 135 ゲートウェイ (GW)
- 22, 32, 42, 52, 62, 124, 126, 134, 136 部門ネットワーク
- 46 NAT
- 51 ホームエージェント (HA)
- 72 ファイアウォール (FW)
- 73 ルータ
- 75 リモートアクセス用ネットワーク
- 111, 121, 131 企業ネットワーク

【書類名】 図面

【図 1】



【図 2】



【図 3】

発信アドレス	宛先アドレス
AD03	AD31
AD43	AD31
AD02	AD20

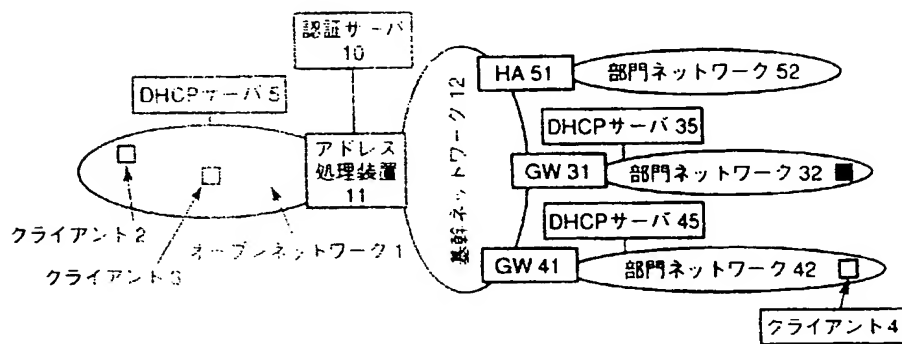
【図 4】

	トンネル発信アドレス	トンネル宛先アドレス		発信アドレス	宛先アドレス
	カプセル化ヘッダ				
(1)	AD03	AD11		AD3X	ADXY
(2)	AD03	AD31		AD3X	ADXY
(3)	AD31	AD03		ADXY	AD3X
(4)	AD11	AD03		ADXY	AD3X

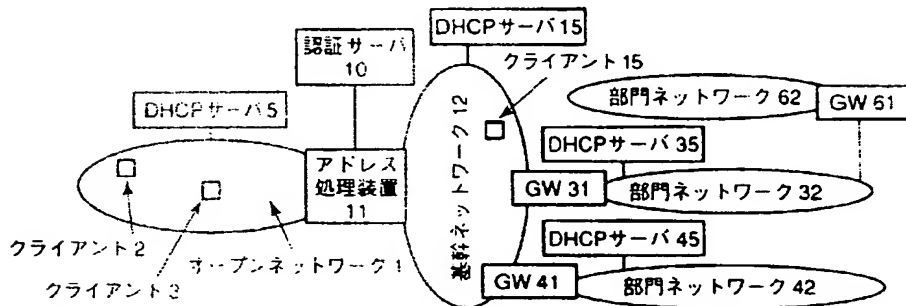
【図 5】

	発信アドレス	宛先アドレス	
(1)	AD02	AD11	
(2)	AD02	AD20	
(3)	AD20	AD02	
(4)	AD11	AD02	

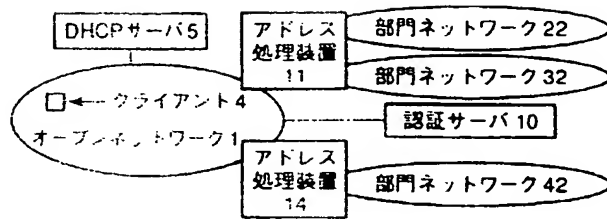
【図 6】



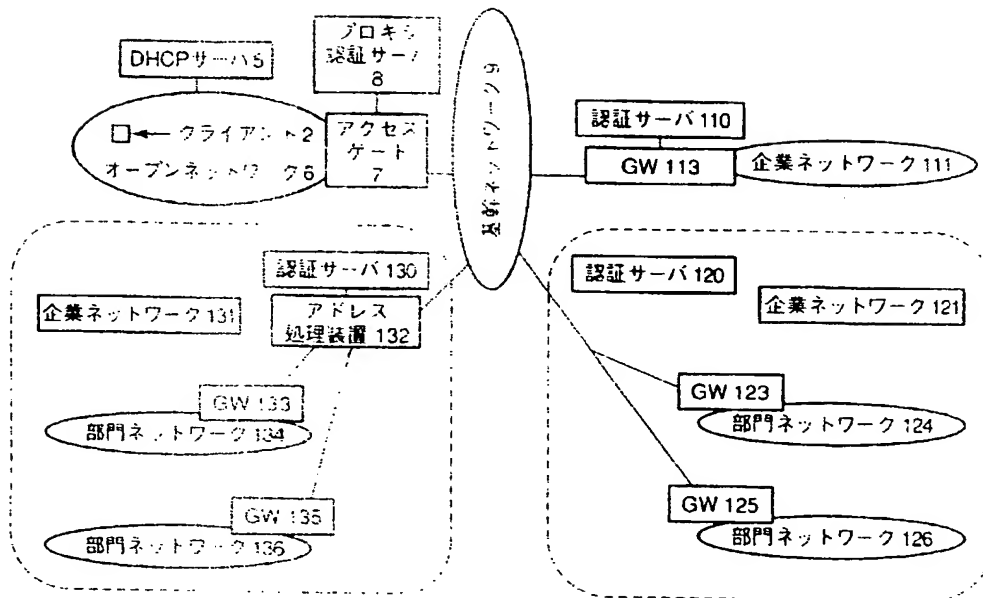
【図 7】



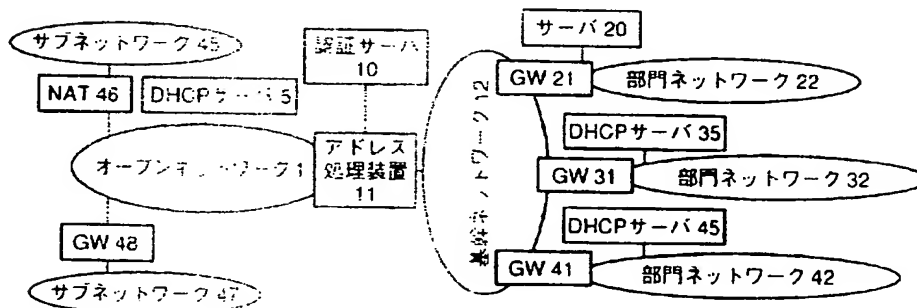
【図 8】



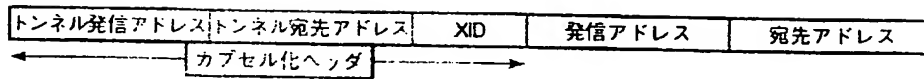
【図 9】



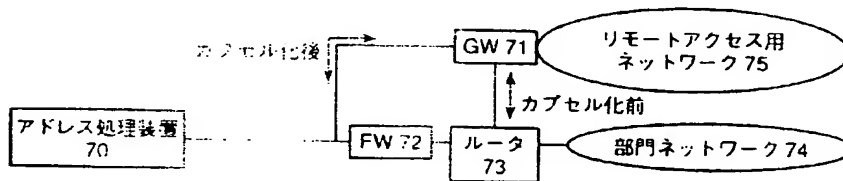
【図 10】



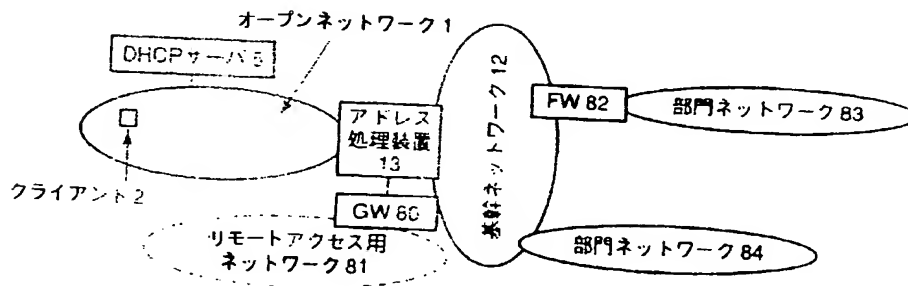
【図 1 1】



【図 1 2】



【図 1 3】



【図 1 4】

	トンネル発信アドレス	トンネル宛先アドレス		発信アドレス	宛先アドレス
	カプセル化ヘッダ				
(1)	AD02	AD13		AD8X	ADXY
(2)	AD02	AD80		AD8X	ADXY
(3)	AD80	AD02		ADXY	AD8X
(4)	AD13	AD02		ADXY	AD8X

【書類名】 要約書

【要約】

【課題】 クライアントの数が増大しても設定や運用管理をシンプルにすること、高いセキュリティ性を実現すること、I P s e c 技術を用いたトンネルをターゲットとなるサブネットワークまで伸張すること。

【解決手段】 認証サーバ 1 0 は、例えば、オープンネットワーク 1 内のクライアント 3 が部門ネットワーク 3 2 にアクセスする際に、クライアント 3 の認証要求に応じてクライアント 3 の認証を行う。アドレス処理回路 1 1 は、認証サーバ 1 0 によるクライアント 3 の認証後に、認証サーバ 1 0 からの指示に基づいて、クライアント 3 と部門ネットワーク 3 2 との間のパケット通信に係るパケット信号のアドレス処理を行う。

【選択図】 図 1

特願 2 0 0 3 - 1 1 5 6 1 8

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 4 2 3 7]

1. 変更年月日	1 9 9 0 年 8 月 2 9 日
[変更理由]	新規登録
住 所	東京都港区芝五丁目 7 番 1 号
氏 名	日本電気株式会社